

Any multipartite entangled state violating Mermin-Klyshko inequality can be distilled for almost all bipartite splits

Soojoon Lee,¹ Jinhyoung Lee,² and Jaewan Kim³

¹ *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea*

² *Department of Physics, Hanyang University, Seoul 133-791, Korea*

³ *School of Computational Sciences, Korea Institute for Advanced Study, Seoul 130-722, Korea*

(Dated: February 7, 2009)

We study the explicit relation between violation of Bell inequalities and bipartite distillability of multi-qubit states. It has been shown that even though for $N \geq 8$ there exist N -qubit bound entangled states which violates a Bell inequality [Phys. Rev. Lett. **87**, 230402 (2001)], for all the states violating the inequality there exists at least one splitting of the parties into two groups such that pure-state entanglement can be distilled [Phys. Rev. Lett. **88**, 027901 (2002)]. We here prove that for all N -qubit states violating the inequality the number of distillable bipartite splits increases exponentially with N , and hence the probability that a randomly chosen bipartite split is distillable approaches one exponentially with N , as N tends to infinity. We also show that there exists at least one N -qubit bound entangled state violating the inequality if and only if $N \geq 6$.

PACS numbers: 03.67.Mn 03.65.Ud, 42.50.Dv

Entanglement has been considered as a key ingredient for quantum information science, and has brought a lot of its useful applications such as quantum key distribution and teleportation. Nevertheless, there still exist open problems related to entanglement, in particular, multipartite entanglement.

It is known that entanglement can be divided into two kinds of entanglement. One is called the *distillable* entanglement, from which some pure entanglement can be extracted by local quantum operations and classical communication, and the other is called the *bound* entanglement, which is not distillable. Since only pure entanglement is directly useful for quantum information processing, the bound entanglement seems to be useless. However, it has been recently shown that any bound entangled (BE) states are useful in quantum teleportation [1, 2], all multipartite pure entangled states are interconvertible by stochastic local operations and classical communication with the assistance of BE states [3], and there are several classes of BE states with a positive key rate in quantum key distribution [4, 5, 6, 7, 8]. Thus, it is necessary to analyze BE states more profoundly.

If one of the two most significant features related to entanglement is distillability, then the other is *nonlocality*, which can be described as a physical property to explain that quantum correlation is quite different from classical correlations. Nonlocality can be seen from violation of some conditions, called Bell inequalities, that are satisfied by any local variable theory, and it is a well-known fact that any bipartite or multipartite pure state violates a Bell inequality if and only if the state is entangled [9, 10]. However, for mixed states, there does not exist such a simple relation between nonlocality and entanglement. Since Werner [11] found the existence of entangled mixed states described by a local hidden variable model, it has been known that some of these states can violate Bell inequalities after appropriately preprocessing the state [12, 13].

There is a simple relation between nonlocality and distillability in fewer-qubit systems: If any two-qubit [14] or three-qubit [15] (pure or mixed) state violates a specific form of the Bell inequality then it is distillable. However, Dür [16] has shown that for $N \geq 8$ there exist N -qubit BE states which violate a Bell inequality. This result seems to show that nonlocality does not directly imply distillability in multipartite cases, even though it has been recently shown that asymptotic violation of a Bell inequality is equivalent to distillability in any multipartite quantum system [17].

But, Acín [18] has demonstrated that for all the states violating the inequality there exists at least one splitting of the parties into two groups such that pure-state entanglement can be distilled, and has more analyzed the relation of nonlocality to bipartite distillability in his subsequent works [19]. This does not only imply that there still exists a relation between nonlocality and distillability for a certain bipartite split, but also tells us that it is possible to make two-party quantum communications with respect to the bipartite split secure against eavesdropping. Then some questions naturally arise such as which bipartite split is distillable and how many splits are possible to be distillable if the Bell inequality is violated.

Assume that a multipartite entangled state violates the Bell inequality. If it could be distilled for almost all bipartite splits, then it would be possible for almost all two-party quantum communications over the multipartite state to be secure against eavesdropping, regardless of how it is divided into two parties. Thus, it would be important to answer the questions in quantum communication theory as well as in entanglement theory.

In this paper, we show that if any N -qubit state violates the inequality then there exist much more than one distillable bipartite splits, to be exact, at least $\lfloor 2^{N-1} - 2^{(N-1)/2} + 1 \rfloor$ distillable bipartite splits. Hence, the distillation probability that a randomly chosen bipartite split is distillable approaches one exponentially with

N as N tends to infinity. This means that if a given N -qubit state violates the Bell inequality for sufficiently large N then almost all bipartite splits are distillable. Furthermore, this result provides us with the following necessary and sufficient condition for the existence of N -qubit BE states violating the inequality: At least one N -qubit BE state violates the inequality if and only if $N \geq 6$.

Since it has been already known that there exists a four-qubit BE state, the so-called Smolin state [20], violating some other Bell inequality [21], our condition does not seem to be very strong. However, because our proof is based on the first main result counting distillable bipartite splits, this justifies some significance of considering the counting problem.

In order to introduce our main results, we first consider the family of N -qubit states ρ_N presented in [22, 23],

$$\rho_N = \sum_{\sigma=\pm} \lambda_0^\sigma |\Psi_0^\sigma\rangle\langle\Psi_0^\sigma| + \sum_{j=1}^{2^{N-1}-1} \lambda_j (|\Psi_j^+\rangle\langle\Psi_j^+| + |\Psi_j^-\rangle\langle\Psi_j^-|), \quad (1)$$

where

$$|\Psi_j^\pm\rangle = \frac{1}{\sqrt{2}} (|j\rangle|0\rangle \pm |2^{N-1}-j-1\rangle|1\rangle), \quad (2)$$

and $\lambda_0^+ + \lambda_0^- + 2 \sum_j \lambda_j = 1$. We remark that any arbitrary N -qubit state can be depolarized to a state in this family, and hence this family can be useful to find sufficient conditions for nonseparability and distillability in N -qubit systems [22]. Thus, this family may be regarded as a generalization of Werner states to multiqubit systems.

We prove our first main result in the following way: (i) We assume that any N -qubit state ρ violates a specific form of Bell inequality. (ii) By some appropriate depolarizing process, the state ρ can be transformed into ρ_N , which also violates the same inequality. (iii) We show that the state ρ_N violating the inequality has at least $\lfloor 2^{N-1} - 2^{(N-1)/2} + 1 \rfloor$ distillable bipartite splits. (iv) We conclude that the state ρ also has at least $\lfloor 2^{N-1} - 2^{(N-1)/2} + 1 \rfloor$ distillable bipartite splits. In order to prove the main result, we need the following proposition and lemma.

For each $(N-1)$ -bit string $j = j_1 j_2 \cdots j_{N-1}$, let P_j be the bipartite split such that $j_i = 0$ if and only if party i belongs to the same set as the last party. Then the following proposition about bipartite distillability of the states ρ_N has been known by Dür and Cirac [23].

Proposition 1. ρ_N is distillable for the bipartite split P_j if and only if $2\lambda_j < \Delta \equiv \lambda_0^+ - \lambda_0^-$.

We note that the quantity Δ in Proposition 1 plays an important role in not only bipartite distillability but also a certain form of Bell inequality, which we will crucially use in this paper.

From Proposition 1, we can obtain the following key lemma for our first main result.

Lemma 2. If

$$\Delta > \frac{1}{2^{(N-1)/2}} \quad (3)$$

then there exist at least $\lfloor 2^{N-1} - 2^{(N-1)/2} + 1 \rfloor$ distillable bipartite splits in ρ_N .

Proof. Let m be the number of distillable bipartite splits, $P_{j_1}, P_{j_2}, \dots, P_{j_m}$. Suppose that $m \leq 2^{N-1} - 2^{(N-1)/2}$. Then we readily obtain the following inequality:

$$\begin{aligned} 1 - \Delta &\geq 2 \sum_{j=1}^{2^{N-1}-1} \lambda_j \\ &= 2(\lambda_{j_1} + \lambda_{j_2} + \cdots + \lambda_{j_m}) + 2 \sum_{j \notin \{j_1, \dots, j_m\}} \lambda_j \\ &\geq 2(\lambda_{j_1} + \lambda_{j_2} + \cdots + \lambda_{j_m}) + (2^{N-1} - 1 - m)\Delta. \end{aligned} \quad (4)$$

It follows that

$$\begin{aligned} 1 &\geq 2(\lambda_{j_1} + \lambda_{j_2} + \cdots + \lambda_{j_m}) + (2^{N-1} - m)\Delta \\ &> 2(\lambda_{j_1} + \lambda_{j_2} + \cdots + \lambda_{j_m}) + (2^{N-1} - m)/2^{(N-1)/2} \\ &\geq 2(\lambda_{j_1} + \lambda_{j_2} + \cdots + \lambda_{j_m}) + 1. \end{aligned} \quad (5)$$

The inequality (5) leads to a contradiction. Therefore, we can conclude that $m > 2^{N-1} - 2^{(N-1)/2}$. \square

The Bell inequality that Dür and Acín have considered is called the Mermin-Klyshko (MK) inequality [24, 25], which generalizes the Clauser-Horne-Shimony-Holt inequality [26] into N -qubit cases. Let \mathcal{B}_N be the Bell operator defined recursively as

$$\mathcal{B}_i = \frac{1}{2} [\mathcal{B}_{i-1} \otimes (\sigma_{\hat{n}_i} + \sigma_{\hat{n}'_i}) + \mathcal{B}'_{i-1} \otimes (\sigma_{\hat{n}_i} - \sigma_{\hat{n}'_i})], \quad (6)$$

where $\sigma_{\hat{n}_i} = \hat{n}_i \cdot \sigma$ and $\sigma_{\hat{n}'_i} = \hat{n}'_i \cdot \sigma$ are the two dichotomic observables measured on each particle i , \mathcal{B}'_i is obtained from \mathcal{B}_i by exchanging all the \hat{n}_i and \hat{n}'_i , and $\mathcal{B}_1 = \sigma_{\hat{n}_1}$. Then the MK inequality is as follows:

$$|\text{tr}(\mathcal{B}_N \rho)| \leq 1. \quad (7)$$

Choosing the same measurement directions in all N locations, $\sigma_{\hat{n}_i} = \sigma_x$ and $\sigma_{\hat{n}'_i} = \sigma_y$ for all i , after local phase redefinition [18], \mathcal{B}_N can be written as

$$\mathcal{B}_N = 2^{(N-1)/2} (|\Psi_0^+\rangle\langle\Psi_0^+| - |\Psi_0^-\rangle\langle\Psi_0^-|). \quad (8)$$

We note that, by the depolarizing process in [22], any N -qubit state ρ can be transformed into one in the family of ρ_N with $\lambda_0^\pm = \langle\Psi_0^\pm|\rho_N|\Psi_0^\pm\rangle = \langle\Psi_0^\pm|\rho|\Psi_0^\pm\rangle$ and $2\lambda_j = \langle\Psi_j^+|\rho_N|\Psi_j^+\rangle + \langle\Psi_j^-|\rho_N|\Psi_j^-\rangle = \langle\Psi_j^+|\rho|\Psi_j^+\rangle + \langle\Psi_j^-|\rho|\Psi_j^-\rangle$. Thus, for the Bell operator \mathcal{B}_N in Eq. (8), we obtain the following equalities:

$$\begin{aligned} 2^{-(N-1)/2} \text{tr}(\mathcal{B}_N \rho) &= \langle\Psi_0^+|\rho|\Psi_0^+\rangle - \langle\Psi_0^-|\rho|\Psi_0^-\rangle \\ &= \langle\Psi_0^+|\rho_N|\Psi_0^+\rangle - \langle\Psi_0^-|\rho_N|\Psi_0^-\rangle \\ &= \lambda_0^+ - \lambda_0^- = \Delta, \end{aligned} \quad (9)$$

and hence we have the following theorem by Lemma 2.

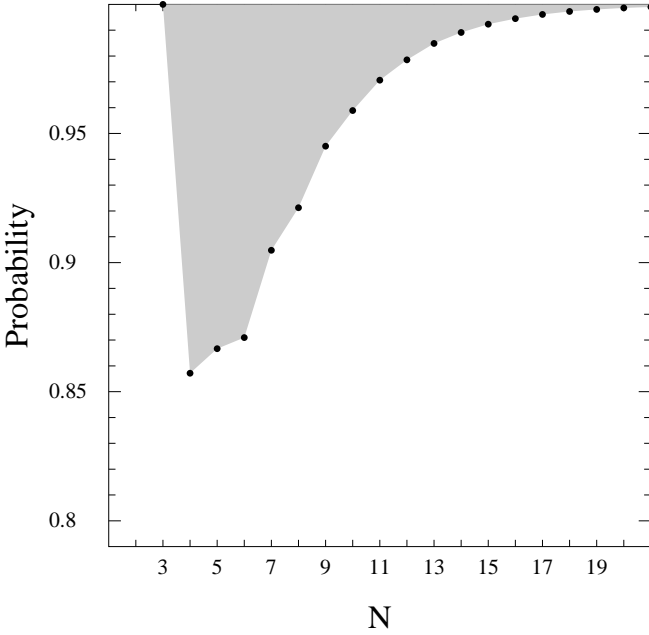


FIG. 1: The distillation probability $P(N)$ that a randomly chosen bipartite split on an N -qubit state is distillable, when it violates the MK inequality with respect to the Bell operator (8).

Theorem 3. *For all the N -qubit states ρ violating the MK inequality with respect to the Bell operator (8), there exist at least $\lfloor 2^{N-1} - 2^{(N-1)/2} + 1 \rfloor$ distillable bipartite splits.*

Let $P(N)$ be the probability that a randomly chosen bipartite split on an N -qubit state is distillable, when it violates the MK inequality with respect to the Bell operator (8). Then it follows from Theorem 3 that

$$P(N) \geq \frac{2^{N-1} - 2^{(N-1)/2}}{2^{N-1} - 1} = 1 - \frac{1}{2^{(N-1)/2} + 1}. \quad (10)$$

This implies that $P(N)$ approaches one exponentially with N as N tends to infinity as seen in FIG. 1.

Interestingly, Theorem 3 provides us with a necessary and sufficient condition for the existence of N -qubit BE states violating the MK inequality with respect to the Bell operator (8). In order to show the condition, we begin with reminding the following proposition about a relation between distillability and negative partial transposition (NPT), which has been shown by Dür and Cirac [22].

Proposition 4. *A maximally entangled pair between particles i and j can be distilled from ρ_N if and only if all possible bipartite splits of ρ_N where the particles i and j belong to different parties, have NPT.*

By Theorem 3 and Proposition 4, we can prove the following theorem.

Theorem 5. *There exists at least one N -qubit BE state violating the MK inequality with respect to the Bell operator (8) if and only if $N \geq 6$.*

Proof. We note that the number of total bipartite splits is $2^{N-1} - 1$, and that the number of all distillable bipartite splits is at least $\lfloor 2^{N-1} - 2^{(N-1)/2} + 1 \rfloor$ by Theorem 3.

We first assume that $N \leq 5$, that is, $N = 3, N = 4$, or $N = 5$.

(Case 1) $N = 3$; It follows from Theorem 3 that all bipartite splits are distillable, and so have NPT. By Proposition 4, a maximally entangled state can be distilled between any particles i and j .

(Case 2) $N = 4$; Since $\lfloor 2^3 - 2^{3/2} + 1 \rfloor = 6$ and $2^3 - 1 = 7$, we obtain that all bipartite splits are distillable or there is only one non-distillable bipartite split. Hence, there is at least one pair i and j such that all bipartite splits whose two different parties contain the particles i and j respectively are distillable. As in the Case 1, since they have NPT, a maximally entangled pair can be distilled between the particles i and j .

(Case 3) $N = 5$; Since $\lfloor 2^4 - 2^2 + 1 \rfloor = 13$ and $2^4 - 1 = 15$, we obtain that all bipartite splits are distillable, or there exist at most two non-distillable bipartite splits. Hence, there is at least one pair i and j between which a maximally entangled pair can be distilled by the same reason as the Case 2.

Conversely, if $N \geq 6$ then there exists an N -qubit BE state violating the MK inequality as follows: Take $\lambda_0^+ = 1/(N-1)$, $\lambda_0^- = 0$, and $\lambda_j = 1/2(N-1)$ if $j = 3, 6, \dots, 3 \cdot 2^{N-3}$ and $\lambda_j = 0$ otherwise. Under these conditions, the state ρ_N becomes,

$$\begin{aligned} \varrho_N = & \frac{1}{N-1} |\Psi_0^+\rangle \langle \Psi_0^+| \\ & + \frac{1}{2(N-1)} \sum_{j \in J_N} (|\Psi_j^+\rangle \langle \Psi_j^+| + |\Psi_j^-\rangle \langle \Psi_j^-|), \end{aligned} \quad (11)$$

where $J_N = \{3, 6, \dots, 3 \cdot 2^{N-3}\}$. Then since $N-1 < 2^{(N-1)/2}$ if $N \geq 6$, the state ϱ_N violates the MK inequality with respect to the Bell operator (8).

Furthermore, since $\Delta = 2\lambda_j$ if $j \in J_N$, by Proposition 1, the state ϱ_N is not distillable for the bipartite splits P_j for $j \in J_N$.

As seen in FIG. 2, if two different particles k and k' in the state ϱ_N are given then $P_{3 \cdot 2^{N-1-k}}$ or $P_{3 \cdot 2^{N-2-k}}$ is a bipartite split where the two particles belong to different parties, and neither $P_{3 \cdot 2^{N-1-k}}$ nor $P_{3 \cdot 2^{N-2-k}}$ is bipartite distillable, and hence a maximally entangled state between the particles k and k' cannot be distilled. Since k and k' are arbitrary, the state ϱ_N is not distillable, that is, it is BE since it is inseparable. Therefore, there exists an N -qubit BE state ϱ_N violating the MK inequality if $N \geq 6$. \square

As seen in Theorem 5, for $3 \leq N \leq 5$, there exists no N -qubit BE state that violates the inequality. Hence we

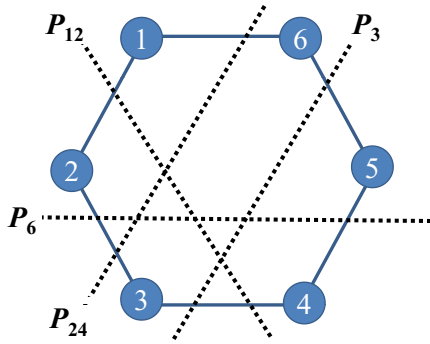


FIG. 2: Undistillable bipartite splits P_j of ϱ_N in (11) when $N = 6$.

can say that if $3 \leq N \leq 5$ then violation of the inequality implies distillability.

In conclusion, we have studied the explicit relation between violation of Bell inequalities and bipartite distillability of multi-qubit states, and have shown that if any N -qubit state violates the MK inequality then there exist at least $\lfloor 2^{N-1} - 2^{(N-1)/2} + 1 \rfloor$ distillable bipartite splits.

Hence, the probability that a randomly chosen bipartite split is distillable approaches one exponentially with N as N tends to infinity. We have also shown that an N -qubit BE state violates the inequality if and only if $N \geq 6$.

It has been shown that while N -qubit states in a class of BE states presented in [16, 18] violate the MK inequality for $N \geq 8$, the states in the class violate different forms of Bell inequalities for $N \geq 7$ in Ref. [27] and for $N \geq 6$ in Ref. [28]. Furthermore, it has been also shown that there exists a four-qubit BE state which can maximally violate a certain form of Bell inequality [21]. Therefore, our results could be also improved by using Bell inequalities different from the MK inequality, and could be furthermore generalized to multipartite distillability.

S.L. was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2007-331-C00049), and J.K. was partially supported by the IT R&D program of MKE/IITA (2005-Y-001-04, Development of Next Generation Security Technology).

-
- [1] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).
 - [2] L. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
 - [3] S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004).
 - [4] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
 - [5] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0506189.
 - [6] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).
 - [7] D.P. Chi, J.W. Choi, J.S. Kim, T. Kim, and S. Lee, Phys. Rev. A **75**, 032306 (2007).
 - [8] P. Horodecki and R. Augusiak, Quantum Information Processing: From Theory to Experiment, D.G. Angelakis *et al.* (eds.), NATO Science Series III, vol. **199**, pp. 19–29, IOS Press, Amsterdam, 2006; arXiv:0712.3999.
 - [9] N. Gisin, Phys. Lett. A **154**, 201 (1991).
 - [10] S. Popescu and D. Rohrlich, Phys. Lett. A **166**, 293 (1992).
 - [11] R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
 - [12] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).
 - [13] N. Gisin, Phys. Lett. A **210**, 151 (1996).
 - [14] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
 - [15] S. Lee, J. Joo, and J. Kim, Phys. Rev. A **76**, 012311 (2007).
 - [16] W. Dür, Phys. Rev. Lett. **87**, 230402 (2001).
 - [17] L. Masanes, Phys. Rev. Lett. **97**, 050503 (2006).
 - [18] A. Acín, Phys. Rev. Lett. **88**, 027901 (2001).
 - [19] A. Acín, V. Scarani, and M.M. Wolf, Phys. Rev. A **66**, 042323 (2002); J. Phys. A: Math. Gen. **36**, L21 (2003).
 - [20] J.A. Smolin, Phys. Rev. A **63**, 032306 (2001).
 - [21] R. Augusiak and P. Horodecki, Phys. Rev. A **74**, 010305(R) (2006).
 - [22] W. Dür, J.I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999); W. Dür and J.I. Cirac, Phys. Rev. A **61**, 042314 (2000).
 - [23] W. Dür and J.I. Cirac, Phys. Rev. A **62**, 022302 (2000).
 - [24] N.D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
 - [25] A.V. Belinski and D.N. Klyshko, Phys. Usp. **36**, 653 (1993).
 - [26] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
 - [27] D. Kaszlikowski, L.C. Kwak, J. Chen, and C.h. Oh, Phys. Rev. A **66**, 052309 (2002).
 - [28] A. Sen(De), U. Sen, and M. Żukowski Phys. Rev. A **66**, 062318 (2002).